Gauss Sums of Cubic Characters over $\mathbb{F}_{p^r}$, p odd

Michele Elia [*], Davide Schipani[†]

November 22, 2011

Abstract

An elementary approach is shown which derives the values of the Gauss sums over $\mathbb{F}_{p^r}$, p odd, of a cubic character. New links between Gauss sums over different field extensions are shown in terms of factorizations of the Gauss sums themselves, which then are revisited in terms of prime ideal decompositions. Interestingly, one of these results gives a representation of primes p of the form $6k+1$ by a binary quadratic form in integers of a subfield of the cyclotomic field of the p-th roots of unity.

Keywords: Gauss sum, character, finite fields, algebraic number fields.

Mathematics Subject Classification (2010): 12Y05, 12E30

1 Introduction

Let $\mathbb{F}_{p^r}$ be a Galois field of order p^r, with $\mathrm{Tr}_r(x) = \sum_{j=0}^{r-1} x^{p^j}$ being the trace function over $\mathbb{F}_{p^r}$, and $\mathrm{Tr}_{r/d}(x) = \sum_{j=0}^{r/d-1} x^{p^{dj}}$ the relative trace function over $\mathbb{F}_{p^r}$ relatively to $\mathbb{F}_{p^d}$, with $d|r$ [16].
Further let χ_m be a character of order m defined over $\mathbb{F}_{p^r}$ and taking values in the cyclotomic field $\mathbb{Q}(\zeta_m)$, where ζ_m denotes a primitive m-th complex root of unity.
The Gauss sum of χ_m over $\mathbb{F}_{p^r}$ is defined, [3, 13], for any $\beta \in \mathbb{F}_{p^r}$ as

$$G_r(\beta, \chi_m) = \sum_{y \in \mathbb{F}_{p^r}} \chi_m(y) \zeta_p^{\mathrm{Tr}_r(\beta y)} = \bar{\chi}_m(\beta) G_r(1, \chi_m) \ .$$

We will focus our interest on cubic characters χ_3 for odd primes p, while the case $p = 2$ is dealt with in [20]. A cubic character χ_3 can be either the principal character, i.e. $\chi_3(\beta) = 1$ for all $\beta \in \mathbb{F}_{p^r}^*$, or a non-principal character (if $p^r \equiv 1 \bmod 6$)

$$\chi_3(\alpha^{h+3j}) = \zeta_3^h \quad h = 0, 1, 2 \ , \ j \in \mathbb{N} \ ,$$

where α is a generator of $\mathbb{F}_{p^r}^*$. In addition, $\chi_3(0) = 0$ by definition.
By the above assumptions, the values of the Gauss sums of a cubic character over $\mathbb{F}_{p^r}$ are in general

[*]Politecnico di Torino, Italy
[†]University of Zurich, Switzerland

algebraic integers in the field $\mathbb{Q}(\zeta_3, \zeta_p) = \mathbb{Q}(\zeta_{3p})$, $p \neq 3$ and $\mathbb{Q}(\zeta_3)$, if $p = 3$. Our aim is to give a thorough overview and derive more precise statements about these values with elementary techniques. In particular, we have obtained an interesting new result in the vein of Gauss' closed expression for $G_1(1, \chi_2)$ in terms of a fourth root of unity and a root of an integral quadratic polynomial. Specifically, our equation (4) expresses $G_1(1, \chi_3)$ in terms of a cubic root of unity and a root of an integral cubic polynomial (see Equation (1)), whose coefficients are given explicit functions of p. Gauss sums over extended fields are obtained from the expression of Gauss sums over smaller fields, either using Davenport-Hasse's theorem or with new methods developed here to link values over different field extensions.

2 Lemmas

For the considerations below, let

$$A_s(\alpha) = \sum_{y \in \mathbb{F}_{p^s}} \chi_m(y + \alpha) \quad \text{and} \quad B_{r,s}(\alpha) = \sum_{z_1 \ldots, z_{r-1} \in \mathbb{F}_{p^s}} \chi_m(1 + \sum_{i=1}^{r-1} z_i \alpha^i) \ ,$$

where α may be in an extension of $\mathbb{F}_{p^s}$, and χ_m defined in the same extension.

Lemma 1 *Let χ_m be a nontrivial character of order m over $\mathbb{F}_{p^{rs}}$, p prime, whose restriction to $\mathbb{F}_{p^s}$ is also nontrivial, and assume that there exists an irreducible polynomial $X^r - \beta$, for a suitable $\beta \in \mathbb{F}_{p^s}$. Then*

$$G_{rs}(1, \chi_m) = \bar{\chi}_m(r) G_s(1, \chi_m) B_{r,s}(\alpha),$$

where α is a root of $X^r - \beta$ (thus with relative trace $\mathrm{Tr}_{rs/s}(\alpha) = 0$).

PROOF. Since $\mathbb{F}_{p^{rs}}$ is an extension of order r of $\mathbb{F}_{p^s}$, its elements can be written in the form $\sum_{i=0}^{r-1} x_i \alpha^i$ with $x_0, \ldots, x_{r-1} \in \mathbb{F}_{p^s}$. We thus have

$$\begin{aligned} G_{rs}(1, \chi_m) &= \sum_{z \in \mathbb{F}_{p^{rs}}} \chi_m(z) \zeta_p^{\mathrm{Tr}_{rs}(z)} = \sum_{x_0, \ldots, x_{r-1} \in \mathbb{F}_{p^s}} \chi_m(\sum_{i=0}^{r-1} x_i \alpha^i) \zeta_p^{\mathrm{Tr}_{rs}(\sum_{i=0}^{r-1} x_i \alpha^i)} \\ &= \sum_{x_0, \ldots, x_{r-1} \in \mathbb{F}_{p^s}} \chi_m(\sum_{i=0}^{r-1} x_i \alpha^i) \zeta_p^{\mathrm{Tr}_s(r x_0)} = \sum_{\substack{x_0 \in F_{p^s}^* \\ x_1 \ldots, x_{r-1} \in \mathbb{F}_{p^s}}} \chi_m(\sum_{i=0}^{r-1} x_i \alpha^i) \zeta_p^{\mathrm{Tr}_s(r x_0)}, \end{aligned}$$

where we used that

$$\mathrm{Tr}_{rs}(\sum_{i=0}^{r-1} x_i \alpha^i) = \mathrm{Tr}_s(\mathrm{Tr}_{rs/s}(\sum_{i=0}^{r-1} x_i \alpha^i)) = \sum_{i=0}^{r-1} \mathrm{Tr}_s(x_i \mathrm{Tr}_{rs/s}(\alpha^i)) = \mathrm{Tr}_s(r x_0) \ ,$$

since, if α is a solution of $X^r - \beta = 0$, then $\mathrm{Tr}_{rs/s}(\alpha^j) = 0$ for every $j = 1, \ldots, r-1$ for example as a consequence of the Newton formulas [4, vol. I, pg. 166]. The sum $\sum_{x_1 \ldots, x_{r-1} \in \mathbb{F}_{p^s}} \chi_m(\sum_{i=1}^{r-1} x_i \alpha^i)$ is zero, since with the change of variable $x_i = x_i' \lambda$, where λ is an element of $\mathbb{F}_{p^s}^*$ with $\chi_m(\lambda) \neq 1$,

the sum becomes $\chi_m(\lambda)\sum_{x_1\ldots,x_{r-1}\in\mathbb{F}_{p^s}}\chi_m(\sum_{i=1}^{r-1}x_i\alpha^i)$.
Now, as $x_0\neq 0$, we may perform the change of variables $x_i=x_0z_i$, $i=1,\ldots,r-1$ and write

$$\begin{aligned} G_{rs}(1,\chi_m) &= \sum_{x_0\in F_{p^s}^*}\zeta_p^{\mathrm{Tr}_s(rx_0)}\sum_{z_1\ldots,z_{r-1}\in\mathbb{F}_{p^s}}\chi_m(x_0+x_0\sum_{i=1}^{r-1}z_i\alpha^i) \\ &= \sum_{x_0\in F_{p^s}^*}\zeta_p^{\mathrm{Tr}_s(rx_0)}\chi_m(x_0)\sum_{z_1\ldots,z_{r-1}\in\mathbb{F}_{p^s}}\chi_m(1+\sum_{i=1}^{r-1}z_i\alpha^i)\ . \end{aligned}$$

The conclusion is immediate, noting that the first summation is simply $\bar{\chi}_m(r)G_s(1,\chi_m)$. □

The following Lemma is a corollary of the previous one, specialized to the case $r=2$. However, we present another proof, whose structure and running results are instrumental to proofs of further theorems.

Lemma 2 *Let χ_m be a nontrivial character of order m over $\mathbb{F}_{p^{2s}}$, p odd, whose restriction to $\mathbb{F}_{p^s}$ is also nontrivial; then*

$$G_{2s}(1,\chi_m)=\chi_m(\alpha)G_s(1,\chi_m)A_s(\frac{1}{2\alpha})\ ,$$

where α is a root of an irreducible polynomial $X^2-\beta$ for a suitable $\beta\in\mathbb{F}_{p^s}$.

We note that from the definition of α and β it follows that $\mathrm{Tr}_{2s/s}(\alpha)=0$ and that $\chi_2(\beta)=-1$ for the nontrivial quadratic character over $\mathbb{F}_{p^s}$.
PROOF. Since $\mathbb{F}_{p^{2s}}$ is a quadratic extension of $\mathbb{F}_{p^s}$, its elements can be written in the form $x+\alpha y$ with $x,y,\in\mathbb{F}_{p^s}$. We thus have

$$G_{2s}(1,\chi_m)=\sum_{z\in\mathbb{F}_{p^{2s}}}\chi_m(z)\zeta_p^{\mathrm{Tr}_{2s}(z)}=\sum_{x,y\in\mathbb{F}_{p^s}}\chi_m(x+\alpha y)\zeta_p^{\mathrm{Tr}_{2s}(x+\alpha y)}=\sum_{x,y\in\mathbb{F}_{p^s}}\chi_m(x+\alpha y)\zeta_p^{\mathrm{Tr}_s(2x)}\ ,$$

where we have used the equality $\mathrm{Tr}_{2s}(x+\alpha y)=2\mathrm{Tr}_s(x)=\mathrm{Tr}_s(2x)$. Multiplying the last sum by $\bar{\chi}_m(2)\chi_m(2)=1$, we can write

$$G_{2s}(1,\chi_m)=\bar{\chi}_m(2)\sum_{x',y\in\mathbb{F}_{p^s}}\chi_m(x'+2\alpha y)\zeta_p^{\mathrm{Tr}_s(x')}\ ,$$

and split the summation into three sums

$$\bar{\chi}_m(2)\sum_{y\in\mathbb{F}_{p^s}}\chi_m(2\alpha y)\ ,\ \bar{\chi}_m(2)\sum_{x'\in\mathbb{F}_{p^s}^*}\chi_m(x')\zeta_p^{\mathrm{Tr}_s(x')}\ ,\ \bar{\chi}_m(2)\sum_{x',y\in\mathbb{F}_{p^s}^*}\chi_m(x'+2\alpha y)\zeta_p^{\mathrm{Tr}_s(x')}\ .$$

The first summation is 0, the second summation is $\bar{\chi}_m(2)G_s(1,\chi_m)$; the third summation can be written as follows: the substitution $y=zx'$ yields

$$\bar{\chi}_m(2)\sum_{x',z\in\mathbb{F}_{p^s}^*}\chi_m(x'+2\alpha zx')\zeta_p^{\mathrm{Tr}_s(x')}=\bar{\chi}_m(2)\sum_{x'\in\mathbb{F}_{p^s}^*}\chi_m(x')\zeta_p^{\mathrm{Tr}_s(x')}\sum_{z\in\mathbb{F}_{p^s}^*}\chi_m(1+2\alpha z)=$$

$$\bar{\chi}_m(2)G_s(1,\chi_m)\chi_m(2\alpha)\sum_{z\in\mathbb{F}_{p^s}^*}\chi_m(z+\frac{1}{2\alpha})=\bar{\chi}_m(2)G_s(1,\chi_m)\chi_m(2\alpha)[A_s(\frac{1}{2\alpha})-\chi_m(\frac{1}{2\alpha})]\ .$$

In conclusion, by combining the above summations, we have $G_{2s}(1,\chi_m)=\chi_m(\alpha)G_s(1,\chi_m)A_s(\frac{1}{2\alpha})$.

□

Corollary 1 *Suppose p is odd and $t = 2^k s$, with $k \geq 1$, and let χ_m be a nontrivial character over $\mathbb{F}_{p^t}$, whose restriction to $\mathbb{F}_{p^s}$ is also nontrivial. Then*

$$G_t(1, \chi_m) = G_s(1, \chi_m) \prod_{i=1}^{k} \chi_m(\alpha_i) A_{2^{i-1}s}(\frac{1}{2\alpha_i}),$$

where α_i is a root of an irreducible polynomial $X^2 - \beta_i$ over $\mathbb{F}_{p^{2^{i-1}s}}$, $i = 1, \ldots, k$.

Lemma 3 *Let χ_m be a character over $\mathbb{F}_{p^s}$, $p \equiv -1$ mod m and m odd. Then $G_s(1, \chi_m)$ is real.*

PROOF. We can write

$$G_s(1, \chi_m) = G_0 + \zeta_m G_1 + \zeta_m^2 G_2 + \cdots + \zeta_m^{m-1} G_{m-1} \ ,$$

where ζ_m is a primitive m-th root of unity and

$$G_j = \sum_{\chi_m(x) = \zeta_m^j} \zeta_p^{\mathrm{Tr}_s(x)} \ , \ 0 \leq j \leq m-1 \ ,$$

known as Gauss periods [11], are real numbers, since $\chi_m(x) = \chi_m(-x)$, as $-1 = (-1)^m$ is an m-th power. Thus, in each sum the exponentials occur in complex conjugated pairs. Furthermore, $G_j = G_{m-j}$ as proved by the following chain of equalities:

$$G_j = \sum_{\chi_m(x) = \zeta_m^j} \zeta_p^{\mathrm{Tr}_s(x)} = \sum_{\chi_m(x) = \zeta_m^j} \zeta_p^{\mathrm{Tr}_s(x^p)} = \sum_{\chi_m(x^p) = \zeta_m^{pj}} \zeta_p^{\mathrm{Tr}_s(x^p)} = \sum_{\chi_m(y) = \zeta_m^{m-j}} \zeta_p^{\mathrm{Tr}_s(y)} = G_{m-j} \ .$$

In fact raising the trace argument to the power p leaves the trace invariant; $\zeta_m^{pj} = \zeta_m^{-j}$ as p is congruent to -1 modulo m; lastly, the automorphism $\sigma(x) = x^p$ simply permutes the elements of the field. Then, for any j, $\zeta_m^j G_j$ and $\zeta_m^{m-j} G_{m-j}$ sum to give a real number, hence $G_s(1, \chi_m)$ is also real.

□

Corollary 2 *Let χ_3 be a cubic character, $p \equiv 2$ modulo 3 ($p = 2$ or $p = 6k + 5$). Then $G_s(1, \chi_3)$ is real.*

Remark 1. For the case $p = 2$, see an alternative proof in [20].

Lemma 4 *Let χ_m be a nontrivial character over $\mathbb{F}_{p^{2s}}$, with p and m odd. If $(p^s - 1, m) = 1$ (in particular the restriction of χ_m to $\mathbb{F}_{p^s}$ is trivial), then $G_{2s}(1, \chi_m) = p^s$.*

PROOF. As in Lemma 2, let α be defined as a root of an irreducible polynomial $X^2 - \beta$, with a suitable $\beta \in \mathbb{F}_{p^s}$. Then

$$G_{2s}(1, \chi_m) = \sum_{x,y \in \mathbb{F}_{p^s}} \chi_m(x + \alpha y) \zeta_p^{\mathrm{Tr}_s(2x)} \ .$$

We split the summation into three: $S_1 = \bar{\chi}_m(2) \sum_{y \in \mathbb{F}_{p^s}} \chi_m(2\alpha y)$,

$$S_2 = \bar{\chi}_m(2) \sum_{x' \in \mathbb{F}_{p^s}^*} \chi_m(x') \zeta_p^{\mathrm{Tr}_s(x')}, \text{ and } S_3 = \bar{\chi}_m(2) \sum_{x', y \in \mathbb{F}_{p^s}^*} \chi_m(x' + 2\alpha y) \zeta_p^{\mathrm{Tr}_s(x')} \ .$$

The first summation is $S_1 = \chi_m(\alpha)(p^s - 1)$, since the character is trivial over $\mathbb{F}_{p^s}$, the second summation is $S_2 = -\bar{\chi}_m(2)$, and the third summation, after the substitution $y = zx'$, gives

$$S_3 = \bar{\chi}_m(2) \sum_{x' \in \mathbb{F}_{p^s}^*} \chi_m(x') \zeta_p^{\mathrm{Tr}_s(x')} \sum_{z \in \mathbb{F}_{p^s}^*} \chi_m(1 + 2\alpha z) = -\bar{\chi}_m(2)[\chi_m(2\alpha) \sum_{z \in \mathbb{F}_{p^s}} \chi_m(\frac{1}{2\alpha} + z) - 1] \ .$$

In order to evaluate $A_s(\frac{1}{2\alpha}) = \sum_{z \in \mathbb{F}_{p^s}} \chi_m(\frac{1}{2\alpha} + z)$, we consider the sum of $A_s(\beta)$, for every $\beta \in \mathbb{F}_{p^{2s}}$, and observe that $A_s(\beta) = p^s - 1$ if $\beta \in \mathbb{F}_{p^s}$, since all elements in this field are m-th powers, while, if $\beta \notin \mathbb{F}_{p^s}$ all sums assume the same value $A_s(\alpha)$, which is shown as follows: set $\beta = u + \alpha v$ with $v \neq 0$, then

$$\sum_{z \in \mathbb{F}_{p^s}} \chi_m(z + u + \alpha v) = \sum_{z \in \mathbb{F}_{p^s}} \chi_m(v) \chi_m((z + u)v^{-1} + \alpha) = \sum_{z' \in \mathbb{F}_{p^s}} \chi_m(z' + \alpha) = A_s(\alpha) \ .$$

Therefore, the sum $\sum_{\beta \in \mathbb{F}_{p^{2s}}} A(\beta) = \sum_{\beta \in \mathbb{F}_{p^{2s}}} \sum_{z \in \mathbb{F}_{p^s}} \chi_m(z + \beta) = \sum_{z \in \mathbb{F}_{p^s}} \sum_{\beta \in \mathbb{F}_{p^{2s}}} \chi_m(z + \beta) = 0$ yields

$$p^s(p^s - 1) + (p^{2s} - p^s)A(\alpha) = 0$$

which implies $A(\alpha) = -1 = A(\frac{1}{2\alpha})$. Finally, by combining the above,

$$G_{2s}(1, \chi_m) = \chi_m(\alpha)(p^s - 1) + \chi_m(\alpha) = \chi_m(\alpha)p^s = p^s \ ,$$

because α, a root of $X^2 - \beta$, is an m-th power, since every $\beta \in \mathbb{F}_{p^s}$ is an m-th power.

□

Remark 2. The above lemma can also be proved using a theorem by Stickelberger, [16, Theorem 5.16] or [22].

3 Results

Trivial character. Let χ_3 be trivial, then

$$G_r(1, \chi_3) = \sum_{y \in \mathbb{F}_{p^r}} \chi_3(y) \zeta_p^{\mathrm{Tr}_r(y)} = \sum_{y \in \mathbb{F}_{p^r}} \zeta_p^{\mathrm{Tr}_r(y)} - 1 = p^{r-1} \sum_{a \in \mathbb{F}_p} \zeta_p^a - 1 = -1 \ ,$$

since the number of elements with the same trace $a \in \mathbb{F}_p$ (0 included) is equal to p^{r-1}, i.e. the number of roots in $\mathbb{F}_{p^r}$ of the equation $\mathrm{Tr}_r(x) = a$. This result settles in particular all the cases of the fields $\mathbb{F}_{3^r}$, or $\mathbb{F}_{p^r}$ with $p \equiv 5 \bmod 6$ and odd r, where there is only the principal character, because every field element is a cube.

Nontrivial character: case p=6k+5. If $p = 6k + 5$ and r is even, a nontrivial cubic character exists and it will be shown that $G_r(1, \chi_3) = -(-p)^{r/2}$, without recurring to Davenport-Hasse's theorem.

Theorem 1 *If $p = 6k + 5$ and s is odd, then $G_{2s}(1, \chi_3) = p^s$.*

PROOF. Since $p^s = -1 \bmod 3$, the conclusion is a consequence of Lemma 4.

□

Theorem 2 *If $p = 6k + 5$ and s is even, then $G_{2s}(1, \chi_3) = (-p)^{s/2} G_s(1, \chi_3)$.*

PROOF. Let $\alpha \in \mathbb{F}_{p^{2s}}$ be a cube and root of an irreducible polynomial $X^2 - \beta$ over $\mathbb{F}_{p^s}$ (clearly such an α exists, since if γ is a root of $X^2 - \beta$, with $\chi_2(\beta) = -1$, then γ^3, a cube, is a root of $X^2 - \beta^3$ and $\chi_2(\beta^3) = \chi_2(\beta)^3 = -1$). Then by Lemma 2

$$G_{2s}(1, \chi_3) = G_s(1, \chi_3) A_s(\frac{1}{2\alpha}) \ ,$$

where $A_s(\frac{1}{2\alpha}) = \sum_{z \in \mathbb{F}_{p^s}} \chi_3(\frac{1}{2\alpha} + z)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_3)$ which can be written as $A_0 + \zeta_3 A_1 + \zeta_3^2 A_2$, where A_0, A_1, and A_2 are the numbers of z for which $\chi_3(\frac{1}{2\alpha} + z)$ is equal to 1, ζ_3 or ζ_3^2, respectively, and $A_0 + A_1 + A_2 = p^s$.

Now, by Lemma 3, both $G_{2s}(1, \chi_3)$ and $G_s(1, \chi_3)$ are real, which implies that $A_s(\frac{1}{2\alpha})$ is also real, so that $A_1 = A_2$. We also know that $A_0 + A_1 + A_2 = A_0 + 2A_1 = p^s$, so we consider two equations for A_0 and A_1:

$$\begin{cases} A_0 + 2A_1 = p^s \\ A_0 - A_1 = \pm p^{s/2} \end{cases}$$

obtained from the fact that we know the absolute values of $G_s(1, \chi_3)$ and $G_{2s}(1, \chi_3)$, [3, Theorem 1.1.4, pg. 10], [20].
Solving for A_1 we have $A_1 = \frac{1}{3}(p^s \mp p^{s/2})$. As A_1 must be an integer, we have

$$A_s(\frac{1}{2\alpha}) = A_0 - A_1 = \begin{cases} p^{s/2} & \text{if } s/2 \text{ is even} \\ -p^{s/2} & \text{if } s/2 \text{ is odd.} \end{cases}$$

□

Corollary 3 *If $p = 6k + 5$ and s is even, then $G_{2s}(1, \chi_3) = -p^s$.*

Nontrivial character: case p=6k+1. If $p = 6k+1$, $p^r - 1$ is divisible by 3, so there exists a nontrivial cubic character in $\mathbb{F}_{p^r}$ for every $r \geq 1$: we know that the Gauss sum over $\mathbb{F}_p$ of a nontrivial cubic character is an algebraic integer in $\mathbb{Q}(\zeta_{3p})$ of absolute value $\sqrt{p}$. Specifically we have

Theorem 3 *If $p = 6k + 1$, then $G_1(1, \chi_3)$ is an element of $\mathbb{Q}(\zeta_3, \eta)$, a subfield of $\mathbb{Q}(\zeta_{3p})$ with degree 6 over $\mathbb{Q}$, where η is a root of a cubic polynomial with rational integer coefficients and cyclic Galois group over $\mathbb{Q}$.*

PROOF. As in the proof of Lemma 3, for a cubic character we can write

$$G_1(1,\chi_3) = G_0 + \zeta_3 G_1 + \zeta_3^2 G_2 \ ,$$

where ζ_3 is a primitive cube root of unity and, for $0 \le j \le 2$,

$$G_j = \sum_{\chi_3(x)=\zeta_3^j} \zeta_p^x \ ,$$

which are real numbers since $\chi_3(x) = \chi_3(-x)$, as -1 is a cubic power. Then, to evaluate the Gauss sum $G_1(1,\chi_3)$ is tantamount to computing the Gauss periods G_0, G_1, and G_2. The following derivation can be found partly, in different form, in Gauss [11, art. 350-352].

Let a be any positive integer less than p and $\sigma_a \in \mathfrak{G}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be the element of the Galois group of $\mathbb{Q}(\zeta_p)$ whose action on ζ_p is defined as $\sigma_a(\zeta_p) = \zeta_p^a$, [23], then

$$\sigma(G_j) = \sum_{\chi_3(x)=\zeta_3^j} \zeta_p^{ax} = \sum_{\chi_3(x'a^{-1})=\zeta_3^j} \zeta_p^{x'} = \sum_{\chi_3(x')=\zeta_3^j\chi_3(a)} \zeta_p^{x'} \ .$$

This implies that any of these automorphisms induces a permutation of G_0, G_1, and G_2, and therefore leaves their symmetric functions invariant, which thus belong to $\mathbb{Q}$. In particular, the three elementary symmetric functions

$$s_1 = G_0 + G_1 + G_2 \ , \ \ s_2 = G_0G_1 + G_1G_2 + G_2G_1 \ , \ \ s_3 = G_0G_1G_2 \ ,$$

are rational integers; it follows that G_0, G_1, and G_2 are the roots of a cubic polynomial with rational coefficients $q(z) = z^3 - s_1z^2 + s_2z - s_3$, which has a cyclic Galois group of order 3 (since $\frac{p-1}{3}$ values of a give the same permutation of its roots). Thus $q(z)$ is irreducible over $\mathbb{Q}$, and denoting one root with η, the other roots can be expressed as polynomials with integer coefficients $r_1(\eta)$ and $r_2(\eta)$ of degree 2 in η.

□

Gauss computed the coefficients of the cubic polynomial $q(z)$ by a clever manipulation of the periods, a task that generally has non-polynomial-time complexity in p. The following theorem proves that these coefficients can be computed, with deterministic polynomial-time complexity, exploiting pure arithmetic features of p without dealing with Gauss periods.

Theorem 4 *Let $q(z)$ be the monic polynomial whose roots are G_0, G_1 and G_2. Then*

$$q(z) = z^3 + z^2 - \frac{p-1}{3}z - \frac{(3+u)p-1}{27}, \tag{1}$$

where u is obtained from the representation $4p = u^2 + 27v^2$ and taken with the sign making the constant term an integer.

PROOF. Let $q(z)$ be as above $z^3 - s_1z^2 + s_2z - s_3$. It is immediately seen that $s_1 = -1$, as $\sum_{x=0}^{p-1} \zeta_p^x = 0$. Using the structure constants of the integral algebra generated by G_0, G_1, and G_2, we will show that $s_2 = -\frac{p-1}{3}$, while s_3 ultimately depends on the representation (u,v) of $4p$ by the quadratic

form $u^2 + 27v^2$.
Let σ be a generator of the cyclic Galois group of $\mathbb{Q}(\eta)$ (σ is also a generator of the Galois group of $q(z)$), then $G_0 = \eta$, $G_1 = \sigma(\eta)$, and $G_2 = \sigma^2(\eta)$ are $\mathbb{Q}$-linearly independent [2] and generate an algebra, [19, Lemma 2.2], whose constants of multiplication [9] are rational integers, [19, Remark 2.3], so that G_0G_1, G_1G_2, and G_2G_0 are linear combinations of G_0, G_1, and G_2 with integer coefficients. Furthermore, since G_0, G_1, and G_2 are cyclically permuted by the action of σ, we can write

$$\begin{cases} G_0G_1 = aG_0 + bG_1 + cG_2 \\ G_1G_2 = aG_1 + bG_2 + cG_0 \\ G_2G_0 = aG_2 + bG_0 + cG_1 \end{cases} \tag{2}$$

where a, b, c are integers whose sum is $\frac{p-1}{3}$, since each G_j contains $\frac{p-1}{3}$ powers of ζ_p and each G_iG_j, $i \neq j$, expands into $\frac{(p-1)^2}{9}$ terms which are powers of ζ_p whose exponents, reduced modulo p, are never 0. Then, summing the three equations, we get

$$s_2 = (a + b + c)(G_0 + G_1 + G_2) = -\frac{p-1}{3} \ .$$

The evaluation of s_3 requires the explicit knowledge of c: by summing the three equations, multiplied by G_2, G_0, and G_1 respectively, we obtain the relation

$$3G_0G_1G_2 = (a + b)s_2 + c(G_0^2 + G_1^2 + G_2^2) = (\frac{p-1}{3} - c)s_2 + c(1 - 2s_2) \ ,$$

which yields $s_3 = \frac{1}{3}[cp - \frac{(p-1)^2}{9}]$. Now, the value of c is specified as follows.
Since the Galois group of $q(z)$, which is a polynomial with integer coefficients, is cyclic of order 3, its discriminant Δ is the square of an integer [6, Proposition 7.4.2]. The direct computation yields

$$\Delta = -\frac{p^2(p^2 - 2p + 1 - 18cp - 18c + 81c^2)}{27} \ ,$$

then Δ must be of the form v^2p^2, whence c is obtained from the equation

$$0 = p^2 - 2p + 1 - 18cp - 18c + 81c^2 + 27u^2 = -4p + (9c - p - 1)^2 + 27v^2 \ . \tag{3}$$

It is known [5, 11, 12, 13] that primes of the form $6k + 1$ are essentially (up to signs) represented in a unique way by the quadratic form $x^2 + 3y^2$ (note that this representation may be computed in deterministic polynomial time using the Schoof algorithm [21] and the Gauss reduction algorithm of quadratic forms [17]). Further, $4 = 1+3$ is represented by the same form, then $4p$ has essentially three different representations, namely

$$4p = (2x)^2 + 3(2y)^2 \quad , \quad 4p = (x - 3y)^2 + 3(x + y)^2 \quad , \quad 4p = (x + 3y)^2 + 3(x - y)^2 \quad .$$

Since x is relatively prime with 3, necessarily exactly one of $2y$, or $x + y$ or $x - y$ is divisible by 3 and allows us to write $4p = u^2 + 27v^2$. By comparison with (3) we have $9c - p - 1 = u$, and u should be taken with the sign that makes the expression $p + 1 + u$ divisible by 9, in order to have an integer c, that is u should be taken with the sign that makes it congruent to 1 modulo 3: since $p+1+u = 0 \bmod 9$ implies that the same expression is 0 modulo 3 and p is congruent to 1 modulo 3, then also u must be congruent 1 modulo 3. □

Corollary 4 *The multiplicative constants of the algebra generated by the periods (equation (2)) are obtained from the representation* $4p = u^2 + 27v^2$ *as*

$$a = \frac{2p - u + 9v - 4}{18} \quad , \quad b = \frac{2p - u - 9v - 4}{18} \quad , \quad c = \frac{p + 1 + u}{9},$$

where the sign of u *is specified in Theorem 4, and the sign of* v *is such that* a *and* b *are compliant with the chosen definitions of* G_1 *and* G_2*.*

PROOF. The value $c = \frac{p+1+u}{9}$ has been found in the proof of Theorem 4, where it was also remarked that $a + b + c = \frac{p-1}{3}$, thus for computing a and b, we only need a further independent relation.
Adding member by member the three equations in (2) after their orderly multiplication by G_0, G_1, G_2, or by G_1, G_2, G_0, respectively, we obtain

$$r_1 = G_0^2 G_1 + G_1^2 G_2 + G_2^2 G_0 = a(G_0^2 + G_1^2 + G_2^2) + (b + c)(G_0 G_1 + G_1 G_2 + G_2 G_0) \ ,$$

$$r_2 = G_1^2 G_0 + G_0^2 G_2 + G_2^2 G_1 = b(G_0^2 + G_1^2 + G_2^2) + (a + c)(G_0 G_1 + G_1 G_2 + G_2 G_0) \ .$$

If we know either r_1, or r_2, then we have a second linear equation for a and b. To compute r_1 and r_2, we observe that they are exchanged by permuting, for example, G_0 and G_1, and are invariant under a cyclic permutation of G_0, G_1, and G_2. Then, their sum $r_1 + r_2$ and product $r_1 r_2$ are symmetric functions of the roots of $q(z)$ and a theorem of Lagrange's [4] assures that they can be expressed by means of the elementary symmetric functions s_1, s_2, and s_3 (the coefficients of $q(z)$). Thus, using properties of the symmetric functions [4], we have

$$r_1 + r_2 = s_1 s_2 - 3s_3 \quad , \quad r_1 r_2 = s_2^3 - 6s_1 s_2 s_3 - 9s_3^2 - s_3 s_1^3 \ ,$$

and substituting the explicit values of s_1, s_2, and s_3 given in Theorem 4, we obtain

$$r_1 + r_2 = \frac{3p - 1 - p(u + 3)}{9} \quad \text{and} \quad r_1 r_2 = \frac{1 + pu + p^2 u^2 - 3p^3}{81} \ .$$

Solving a second degree equation, we find $r_1 = \frac{1}{2}(\frac{3p-1-p(u+3)}{9} + pv)$ and $r_2 = \frac{1}{2}(\frac{3p-1-p(u+3)}{9} - pv)$, where the sign of v should be properly chosen to match the values of r_1 and r_2 obtained from the definition of the Gauss periods. In conclusion, from the system

$$\begin{cases} a + b & = & \dfrac{2p - 4 - u}{9} \\ a\frac{2p+1}{3} - b\frac{p-1}{3} & = & \dfrac{2p^2 + 27pv - pu - 2u - 8}{54} \end{cases}$$

we obtain $a = \frac{2p-u+9v-4}{18}$ and $b = \frac{2p-u-9v-4}{18}$.

□

It is possible to obtain a representation of the Gauss sum $G_1(1, \chi_3)$ in terms of a single root η_p of $q(z)$ by expressing G_0, G_1, and G_2 in terms of η_p, because $\mathbb{Q}(\eta_p)$ is the splitting field of $q(z)$, as seen in Theorem 3 (cf. also [2]). For example, we may set $G_0 = \eta_p$, thus the other roots, that is, Gauss periods, are

$$G_1 = \frac{G_0^2}{v} + \frac{4 - u - 3v}{6v} G_0 + \frac{2 - u - 9v - 4p}{18v} \ ,$$

$$G_2 = -\frac{G_0^2}{v} - \frac{3v-u+4}{6v}G_0 - \frac{9v-u-4p+2}{18v} \ .$$

We note that changing the sign of v is equivalent to exchanging the values of G_1 and G_2. These equations establish a correspondence between G_0, and G_1 and G_2, thus the coefficients a, b, and c in equation (2) can be uniquely specified, for instance the equation $G_0G_1 = aG_0 + bG_1 + cG_2$ is satisfied choosing

$$a = \frac{2p-u-9v-4}{18} \quad \text{and} \quad b = \frac{2p-u+9v-4}{18} \ ,$$

whatever be the sign of v; c is specified in any case as shown in Theorem 4.

These observations yield the following representation:

Theorem 5 *The Gauss sum $G_1(1,\chi_3)$ is uniquely characterized in terms of a root η_p of $q(z)$, with u, v obtained from the representation $u^2 + 27v^2$ of $4p$, as*

$$\eta_p + \zeta_3(\frac{\eta_p^2}{v} + \frac{4-u-3v}{6v}\eta_p + \frac{2-u-9v-4p}{18v}) + \zeta_3^2(-\frac{\eta_p^2}{v} - \frac{3v-u+4}{6v}\eta_p - \frac{9v-u-4p+2}{18v}) \ . \quad (4)$$

Remark 3. Since $\zeta_3^2 = -1-\zeta_3$, we can write

$$G_1(1,\chi_3) = G_0 - G_2 + \zeta_3(G_1 - G_2) \ ,$$

thus the relation $G_1(1,\chi_3)\bar{G}_1(1,\chi_3) = p$ yields

$$p = (G_0-G_2)^2 - (G_0-G_2)(G_1-G_2) + (G_1-G_2)^2$$

which shows that the equation $x^2 - xy + y^2 = p$ has further solutions in the maximal order of $\mathbb{Q}(\zeta_p)$ besides the solutions in rational integers, for example $x = r_1(\eta) - \eta$ and $y = r_2(\eta) - \eta$.

Example Consider $p = 7$, then the Gauss sum has the form

$$G_1(1,\chi) = (\zeta_7 + \zeta_7^6) + \zeta_3(\zeta_7^2 + \zeta_7^5) + \zeta_3^2(\zeta_7^3 + \zeta_7^4) \ ,$$

the coefficients G_j of the powers of ζ_3 are real, and are roots of the cubic polynomial z^3+z^2-2z-1, which has a cyclic Galois group of order 3 over $\mathbb{Q}$. Let η_7 be a root of this polynomial. The other roots are $-2+\eta_7^2$ and $1-\eta_7-\eta_7^2$, thus if we choose the roots $\eta_7 = \zeta_7 + \zeta_7^6$, and the other two roots equal to $\zeta_7^2+\zeta_7^5$ and $\zeta_7^3+\zeta_7^4$, respectively, we obtain the expression $\eta_7+\zeta_3(-2+\eta_7^2)+\zeta_3^2(1-\eta_7-\eta_7^2)$, which coincides with the expression obtained specializing (4) with $p = 7$, $u = 1$, and $v = 1$. Furthermore, it is direct to check that $x = -2+\eta_7^2-\eta_7$ and $y = 1-\eta_7-\eta_7^2-\eta_7$ give a representation of 7 through the quadratic form $x^2 - xy + y^2$ in integers of $\mathbb{Q}(\eta_7)$, which may be of interest besides the 12 representations in rational integers (see e.g. [13, Proposition 8.3.1], [18]), namely $x = 2$ and $y = -1$ and those obtained through associates and conjugates of $2-\zeta_3$ in $\mathbb{Q}(\zeta_3)$.

A Gauss sum over $\mathbb{F}_{p^r}$ is in general also not rational, as can be found using Davenport-Hasse's theorem, [3, 14], by lifting the case over $\mathbb{F}_p$. If there exists an irreducible polynomial $X^r - \beta$ over $\mathbb{F}_p$ we can use Lemma 1 to obtain the following theorem:

Theorem 6 *If $p = 6k + 1$, and if there exists an irreducible polynomial $X^r - \beta$ over $\mathbb{F}_p$, then $G_r(1, \chi_3)$ is again an element of the subfield $\mathbb{Q}(\zeta_3, \eta)$ of degree 6 of $\mathbb{Q}(\zeta_{3p})$, and in particular it can be written in the form*

$$G_r(1, \chi_3) = \bar{\chi}_3(r) G_1(1, \chi_3) B_{r,1}(\alpha) \ ,$$

where α is a root of $X^r - \beta$. The factor $B_{r,1}(\alpha)$ has the form $B_0 + B_1\zeta_3 + B_2\zeta_3^2$ where B_0, B_1, and B_2 are positive rational integers, that can be computed, up to a permutation, from the solutions of a quadratic Diophantine equation.

PROOF. By Lemma 1, we have

$$G_r(1, \chi_3) = \bar{\chi}_3(r) G_1(1, \chi_3) B_{r,1}(\alpha) \ ,$$

where $B_{r,1}(\alpha)$ is an element of $\mathbb{Q}(\zeta_3)$ with absolute value $\sqrt{p^{r-1}}$ (by taking absolute values of both sides). This expression shows that $G_r(1, \chi_3)$ belongs to $\mathbb{Q}(\eta, \zeta_3)$ as $G_1(1, \chi_3)$, since $B_{r,1}(\alpha)$ belongs to $\mathbb{Q}(\zeta_3)$. The factor $B_{r,1}(\alpha) \in \mathbb{Q}(\zeta_3)$ can be written as

$$B_{r,1}(\alpha) = B_0 + B_1\zeta_3 + B_2\zeta_3^2$$

where B_0, B_1, and B_2 are positive integers whose sum is p^{r-1}. Since the square of the norm of $B_{r,1}(\alpha)$ is p^{r-1}, we have the Diophantine equation

$$p^{r-1} = B_0^2 + B_1^2 + B_2^2 - B_0B_1 - B_1B_2 - B_2B_0 \ .$$

Using the relation $B_0 + B_1 + B_2 = p^{r-1}$, we eliminate B_2 and obtain a quadratic Diophantine equation that can be solved for B_0 and B_1:

$$3B_0^2 + 3B_1^2 + 3B_0B_1 - 3p^{r-1}B_0 - 3p^{r-1}B_1 + 3(p^{2r-1} - p^{r-1}) = 0 \ .$$

With the substitution

$$B_0 = \frac{X + p^{r-1}}{3} \ , \ \ B_1 = \frac{Y + p^{r-1}}{3} \ ,$$

we obtain the equation

$$X^2 + XY + Y^2 - 3p^{r-1} = 0 \ ,$$

whose solutions can be obtained from the solution of

$$u^2 + uv + v^2 = p$$

as coming from

$$X - \zeta_3 Y = (1 - \zeta_3)(u - v\zeta_3)^{r-1}$$

by composition of quadratic forms. The ultimate assignment of the solutions to the B_i depends on the choice of the primitive roots in the definition of the Gauss sums.

□

In the following we focus on the special case $r = 2$ to enlighten some properties and relations of the Gauss sums seen from different perspectives.

Theorem 7 *If $p = 6k+1$, then $G_2(1,\chi_3)$ is again an element of the subfield $\mathbb{Q}(\zeta_3,\eta)$ of degree 6 of $\mathbb{Q}(\zeta_{3p})$, and in particular it can be written in the form*

$$G_2(1,\chi_3) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha}) \ ,$$

where α is a root of $x^2-\beta$ and $\beta \in \mathbb{F}_p$ is a cube and quadratic non-residue.

PROOF. As in Theorem 2, we can find such an α and then use Lemma 2 to deduce

$$G_2(1,\chi_3) = G_1(1,\chi_3)\sum_{z\in\mathbb{F}_p}\chi_3(\frac{1}{2\alpha}+z) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha}) \ ,$$

where $A_1(\frac{1}{2\alpha})$ is an element of $\mathbb{Q}(\zeta_3)$ with absolute value $\sqrt{p}$ and $\chi_3(\alpha)=1$.
In conclusion $G_2(1,\chi_3) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha})$ shows that $G_2(1,\chi_3)$ belongs to $\mathbb{Q}(\eta,\zeta_3)$.

□

Remark 4. Theorem 7 states that the Gauss sum $G_2(1,\chi_3)$ is the product of $G_1(1,\chi_3)$ and $A_1(\frac{1}{2\alpha})$, a result that is slightly different from that obtained using Davenport-Hasse's theorem [13], which states that $G_2(1,\chi_3') = -G_1(1,\chi_3)^2$, where χ_3' is defined by extending the nontrivial character over $\mathbb{F}_p$ to a character over $\mathbb{F}_{p^m}$, using the extension rule

$$\chi_3'(x) = \chi_3(N_{\mathbb{F}_{p^m}}(x)),$$

where $N_{\mathbb{F}_{p^m}}(x) = x\cdot x^p\cdots x^{p^{m-1}}$ is the norm of x. In our case we have $\chi_3'(x) = \chi_3(N_{\mathbb{F}_{p^2}}(x))$, and whenever χ_3' is restricted to $\mathbb{F}_p$, we specifically have

$$\chi_3'(x) = \chi_3(N_{\mathbb{F}_{p^2}}(x)) = \chi_3(x^2) = \bar{\chi}_3(x) \quad \forall x\in\mathbb{F}_p \ .$$

Therefore, since $G_2(1,\bar{\chi}_3') = \chi_3'(-1)\bar{G}_2(1,\chi_3') = \bar{G}_2(1,\chi_3')$, the equation given by Davenport-Hasse can be read as

$$G_2(1,\chi_3') = -\bar{G}_1(1,\chi_3')^2 \ ,$$

where χ_3' is a cubic character defined in $\mathbb{F}_{p^2}$, and $\bar{G}_1(1,\chi_3')$ is evaluated on the subset $\mathbb{F}_p$.
In the following proposition we show how this relation may also be derived elementarily. First we need a well-known lemma (see also [13, Proposition 8.3.3] or [1]), for which we present an alternative proof:

Lemma 5 *If $p = 6k+1$, then $G_1(1,\chi_3)^3 = p\sum_{x\in\mathbb{F}_p}\chi_3(x(x-1))$.*

PROOF. The proof is straightforward from the computation of the cube

$$G_1(1,\chi_3)^3 = \sum_{x,y,z\in\mathbb{F}_p}\chi_3(xyz)\zeta_p^{x+y+z} = \sum_{x,y,u\in\mathbb{F}_p}\chi_3(xy(u-x-y))\zeta_p^u \ ,$$

in which the substitution $u = x+y+z$ has been performed. The summation over x can be split into two summations S_1 and S_2, depending on whether $u=y$ or $u\neq y$. The first summation turns out to be 0, since

$$S_1 = \sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\chi_3(xy\ \ (x))\zeta_p^y = \sum_{y\in\mathbb{F}_p}\chi_3(y)\zeta_p^y\sum_{x\in\mathbb{F}_p}\chi_3(x^2) = \sum_{y\in\mathbb{F}_p}\chi_3(y)\zeta_p^y\sum_{x\in\mathbb{F}_p}\chi_3^2(x) = 0 \ .$$

The second summation, with the substitution $x = x'(u-y)$, becomes

$$S_2 = \sum_{\substack{y,u\in\mathbb{F}_p \\ y\neq u}} \zeta_p^u \sum_{x\in\mathbb{F}_p} \chi_3(xy(u-x-y)) = \sum_{\substack{y,u\in\mathbb{F}_p \\ y\neq u}} \chi_3(y)\zeta_p^u \sum_{x'\in\mathbb{F}_p} \bar{\chi}_3(u-y)\chi_3(x'(1-x')) \ .$$

Defining $A = \sum_{x'\in\mathbb{F}_p} \chi_3(x'(1-x'))$, a constant that does not depend on u or y, we may write

$$S_2 = A \sum_{u\in\mathbb{F}_p} \zeta_p^u \sum_{y\neq u} \chi_3(y)\bar{\chi}_3(u-y) = A[\sum_{y\in\mathbb{F}_p} \chi_3(y)\bar{\chi}_3(0-y) + \sum_{u\neq 0} \zeta_p^u \sum_{y\in\mathbb{F}_p} \chi_3(y)\bar{\chi}_3(u-y)] \ .$$

In conclusion, we have $S_2 = Ap$, since the first summation over y is $p-1$, the second summation over y is -1 independently of u, [20, 24]; finally, the summation over u is -1, so that $p-1+(-1)(-1) = p$.

□

Since $G_1(1,\chi_3)\bar{G}_1(1,\chi_3) = p$, the above result gives

$$G_1(1,\chi_3)^3 = G_1(1,\chi_3)\bar{G}_1(1,\chi_3)A$$

which implies that $G_1(1,\chi_3)^2 = \bar{G}_1(1,\chi_3)A$. On the other hand, Theorem 7 gives

$$G_2(1,\chi_3) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha}) \ ,$$

thus we can prove the identity $G_2(1,\chi_3) = -\bar{G}_1(1,\chi_3)^2$, implied by Davenport-Hasse's theorem, if we can prove that $A = -\bar{A}_1(\frac{1}{2\alpha})$. It is in fact immediately seen that both A and $A_1(\frac{1}{2\alpha})$ are primes of the form $a+b\zeta_3$ and field norm p in $\mathbb{Z}(\zeta_3)$. Less direct is the exact relation between them, which we establish in the following proposition making use of the function defined as

$$F(d,i) = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} \left(\frac{g^i y + d}{p}\right) \ ,$$

where g is a primitive element in $\mathbb{F}_p$.

Proposition 1

$$A = -\bar{A}_1(\frac{1}{2\alpha}) \ .$$

PROOF. We can write A in the following form

$$A = \sum_{x\in\mathbb{F}_p} \chi_3(x(x-1)) = \sum_{z\in\mathbb{F}_p} \chi_3(z^2 - \frac{1}{4}) \ , \tag{5}$$

where the last expression was obtained by making the substitution $x = z+\frac{1}{2}$. Furthermore, $A_1(\frac{1}{2\alpha})$ can be written in a similar form, arguing as follows:

$$\bar{A}_1(\frac{1}{2\alpha}) = \sum_{x\in\mathbb{F}_p} \bar{\chi}_3(x+\frac{1}{2\alpha}) = \sum_{x\in\mathbb{F}_p} \chi_3(x+\frac{1}{2\alpha})^2 \ .$$

Furthermore, the identity $\chi_3(y) = \chi_3(y)^p = \chi_3(y^p)$, which is true since p is congruent to 1 modulo 3 and χ_3 is a multiplicative character, implies

$$\chi_3(x+\frac{1}{2\alpha}) = \chi_3(x+\frac{1}{2\alpha})^p = \chi_3(x^p+\frac{1}{(2\alpha)^p}) = \chi_3(x-\frac{1}{(2\alpha)}) \ ,$$

as x and 2 belong to $\mathbb{F}_p$, α is a root of $x^2-\beta$ and the Frobenius automorphism exchanges the roots. Then

$$\bar{A}_1(\frac{1}{2\alpha}) = \sum_{x\in\mathbb{F}_p} \chi_3(x+\frac{1}{2\alpha})\chi_3(x+\frac{1}{2\alpha}) = \sum_{x\in\mathbb{F}_p} \chi_3(x^2-\frac{1}{4\beta}) \ . \tag{6}$$

We notice now that, by definition, the value of any summation $\sum_{z\in\mathbb{F}_p}\chi_3(z^2-d)$ can be written in the form $a_0+a_1\zeta_3+a_2\zeta_3^2$, where a_0, a_1 and a_2 are the numbers of $z\in\mathbb{F}_p$ such that the value of $\chi_3(z^2-d)$ is either 1, or ζ_3, or ζ_3^2. Therefore, writing $z^2-d=g^iy$, with $\chi_3(y)=1$, we have

$$a_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{g^iy+d}{p}\right)] = \frac{p-1}{3} + F(d,i) \quad i=0,1,2 \ ,$$

since $[1+\left(\frac{g^iy+d}{p}\right)]$ is equal to 0, if g^iy+d is not a square; it is equal to 1 if $g^iy+d=0$; and it is equal to 2 if g^iy+d is a square.
Then, setting $A=b_0+b_1\zeta_3+b_2\zeta_3^2$ and $\bar{A}_1(\frac{1}{2\alpha}) = c_0+c_1\zeta_3+c_2\zeta_3^2$, and using the expressions for A and $\bar{A}_1(\frac{1}{2\alpha})$ given in (5) and (6), we obtain

$$b_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{g^iy+\frac{1}{4}}{p}\right)] \text{ and } c_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{g^iy+\frac{1}{4\beta}}{p}\right)] \quad i=0,1,2 \ .$$

The numbers c_i can be written as follows

$$c_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{g^iy+\frac{1}{4\beta}}{p}\right)] = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1-\left(\frac{\beta}{p}\right)\left(\frac{g^iy+\frac{1}{4\beta}}{p}\right)] = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1-\left(\frac{g^i\beta y+\frac{1}{4}}{p}\right)]$$

because β is a quadratic non-residue; furthermore, since β is a cube, setting $w=y\beta$, we deduce that

$$c_i = \sum_{\substack{w\in\mathbb{F}_p^* \\ \chi_3(w)=1}} [1-\left(\frac{g^iw+\frac{1}{4}}{p}\right)] = \frac{p-1}{3} - F(\frac{1}{4},i) \ ,$$

which only differs in sign from $b_i = \frac{p-1}{3} + F(\frac{1}{4},i)$. The proposition follows from the fact that

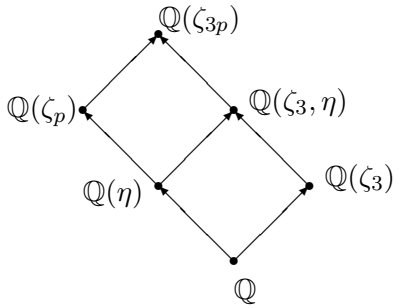
$$A = b_0+b_1\zeta_3+b_2\zeta_3^2 = (b_0-b_2)+(b_1-b_2)\zeta_3$$

and

$$\bar{A}_1(\frac{1}{2\alpha}) = (c_0-c_2)+(c_1-c_2)\zeta_3 = (b_2-b_0)+(b_2-b_1)\zeta_3 \ .$$

□

Remark 5. As has been said, Gauss sums are algebraic integers that belong to a subfield of a cyclotomic field, and in the above theorems we found some factorizations of Gauss sums into elements that may belong to different subfields. For example Theorem 4 shows that $G_2(1,\chi_3) \in \mathbb{Q}(\zeta_3,\eta)$ can be expressed as a product of $G_1(1,\chi_3) \in \mathbb{Q}(\zeta_3,\eta)$ and $A_1(\frac{1}{2\alpha}) \in \mathbb{Q}(\zeta_3)$. The general picture of the fields involved in these factorizations is shown in the following figure



Every extension is Galois, in particular $\mathbb{Q}(\eta)$, $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_3,\eta)$ have Galois groups $\mathfrak{G}(\mathbb{Q}(\eta)/\mathbb{Q})$, $\mathfrak{G}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$, and $\mathfrak{G}(\mathbb{Q}(\zeta_3,\eta)/\mathbb{Q})$, which are cyclic groups of order 3, 2, and 6, respectively; moreover, the third group $\mathfrak{G}(\mathbb{Q}(\zeta_3,\eta)/\mathbb{Q}) = \mathfrak{G}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \times \mathfrak{G}(\mathbb{Q}(\eta)/\mathbb{Q})$ is a direct product of the other two (see also [23]). In these fields, every rational prime p of the form $6k+1$ splits into prime ideals as follows:

$(p) = \mathfrak{p}^3$ in $\mathbb{Q}(\eta)$, i.e. the ideal (p) fully ramifies;

$(p) = (\pi_1)(\pi_2)$ in $\mathbb{Q}(\zeta_3)$, i.e. the ideal (p) fully splits into principal ideals;

$(p) = \mathfrak{P}_1^3\mathfrak{P}_2^3$ in $\mathbb{Q}(\zeta_3,\eta)$, i.e. the ideal (p) fully splits into ramified ideals;

$(\pi_1) = \mathfrak{P}_1^3$ and $(\pi_2) = \mathfrak{P}_2^3$, i.e. the principal ideals of $\mathbb{Q}(\zeta_3)$ fully ramify in $\mathbb{Q}(\zeta_3,\eta)$;

$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$ in $\mathbb{Q}(\zeta_3,\eta)$.

These factorizations can be established by the properties given in [7, pg. 137-138], that is Dedekind's formulation in terms of ideals of a theorem of Kummer's, or in [23, pg. 15].
Let τ_2 denote the automorphism of order 2 in $\mathfrak{G}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$, which leaves the elements of $\mathbb{Q}(\eta)$ invariant when considered as elements of $\mathfrak{G}(\mathbb{Q}(\zeta_3,\eta)/\mathbb{Q})$, then $\tau_2(\mathfrak{P}_1) = \mathfrak{P}_2$.
Now, the Gauss sum $G_1(1,\chi_3)$ is an element of $\mathbb{Q}(\zeta_3,\eta)$ that divides p, as $G_1(1,\chi_3)\bar{G}_1(1,\chi_3) = p$, [3], so that $(G_1(1,\chi_3))(\tau_2(G_1(1,\chi_3))) = (G_1(1,\chi_3))(\bar{G}_1(1,\chi_3)) = (p)$.Therefore the principal ideal $(G_1(1,\chi_3))$ will be a product of powers of the two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$, i.e $(G_1(1,\chi_3)) = \mathfrak{P}_1^a\mathfrak{P}_2^b$, where $a+b=3$ by the unique factorization in prime ideals, since the previous relation gives $(p) = \mathfrak{P}_1^a\mathfrak{P}_2^b\tau_2(\mathfrak{P}_1^a\mathfrak{P}_2^b) = \mathfrak{P}_1^a\mathfrak{P}_2^b\mathfrak{P}_2^a\mathfrak{P}_1^b = \mathfrak{P}_1^{a+b}\mathfrak{P}_2^{a+b}$.
Thus, we may assume that $(G_1(1,\chi_3)) = \mathfrak{P}_1\mathfrak{P}_2^2$, as $G_1(1,\chi_3)$ belongs properly to $\mathbb{Q}(\zeta_3,\eta)$, whence Theorem 7 and Proposition 1 show that $(G_2(1,\chi_3)) = \mathfrak{P}_1^4\mathfrak{P}_2^2 = (\pi_1)\mathfrak{P}_1\mathfrak{P}_2^2$.
In this framework, if the character χ_3' is used, the role of the two prime ideals is simply exchanged, i.e. $(G_2(1,\chi_3')) = \mathfrak{P}_2^4\mathfrak{P}_1^2 = (\pi_2)\mathfrak{P}_2\mathfrak{P}_1^2$, which is the expression defined by Davenport-Hasse's theorem written in terms of ideals.

In general, the Gauss sums $G_s(1,\chi_3)$ for any s can be expressed in terms of ideals as follows: $(G_s(1,\chi_3)) = \mathfrak{P}_2^s\mathfrak{P}_1^{2s}$.
However, these formulations in terms of ideals (see also [8, 15, 22]) conceal the information about which units are involved. In this sense, the elementary direct approach can be more informative, although it may require different approaches for different situations. Considering for example the Gauss sum mentioned above, $G_1(1,\chi)$ for $p = 7$ (see also [10]), setting $\eta_7 = \zeta_7 + \zeta_7^6$, we can explicitly write the expression (which can also be obtained specializing (4) with $p = 7, u = 1, v = 1$)

$$G_1(1,\chi) = \eta_7 + \zeta_3(-2 + \eta_7^2) + \zeta_3^2(1 - \eta_7 - \eta_7^2) \ ,$$

whereas, choosing the ideals $\mathfrak{P}_1 = (\zeta_3 - \eta_7)$, $\mathfrak{P}_2 = (\zeta_3^2 - \eta_7)$, we must find a unit in order to obtain a complete factorization: $G_1(1,\chi) = (4 - \eta_7 - 2\eta_7^2)(\zeta_3 - \eta_7)(\zeta_3^2 - \eta_7)^2$, where $4 - \eta_7 - 2\eta_7^2$ is a unit.

Acknowledgment

The Research was supported in part by the Swiss National Science Foundation under grant No. 132256.

References

[1] S. D. Adhikari, The early reciprocity laws: from Gauss to Eisenstein, *Cyclotomic fields and related topics*, Bhaskaracharya Pratishthana, Pune 2000, pg. 55-74.

[2] E. Artin, *Galois Theory*, Notre Dame University, 1959.

[3] B. Berndt, R. J. Evans, H. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[4] W. S. Burnside, A. W. Panton, *The theory of equations with an introduction to the theory of binary quadratic forms*, Dover, New York, 1960.

[5] H. H. Chan, L. Long, Y. F. Yang, A Cubic Analogue of the Jacobsthal Identity, *Amer. Math. Monthly*, vol. 116, No. 4, 2011, pg. 316-326.

[6] D. A. Cox, *Galois Theory*, Wiley, New York, 2004.

[7] R. Dedekind, *Theory of Algebraic Numbers*, Cambridge, London, 1996.

[8] R. Denomme, A History of Stickelberger's Theorem, *Senior Honors Thesis*, The Ohio State University, 2009.

[9] L. E. Dickson, *Algebras and their Arithmetics*, Dover, 1960.

[10] P. Garrett, *Kummer, Eisenstein, computing Gauss sums as Lagrange resolvents*, http://www.math.umn.edu/~garrett/m/v/kummer_eis.pdf, 2010.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer, New York, 1966.

[12] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 2008.

[13] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1990.

[14] D. Jungnickel, *Finite Fields, Structure and Arithmetics*, Wissenshaftsverlag, Mannheim, 1993.

[15] S. A. Katre, Gauss-Jacobi sums and Stickelberger's theorem, *Cyclotomic fields and related topics*, Bhaskaracharya Pratishthana, Pune 2000, pg. 75-92.

[16] R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.

[17] G. B. Mathews, *Theory of numbers*, Chelsea Pub. Co., 1980.

[18] R. A. Mollin, *Advanced Number Theory with Applications*, CRC Press, Boca Raton (FL), 2010.

[19] C. Monico, M. Elia, An Additive Characterization of Fibers of Characters on $\mathbb{F}_p^*$, *Int. J. Algebra*, Vol. 1-4, n.3, 2010, pg. 109-117.

[20] D. Schipani, M. Elia, Gauss Sums of the Cubic Character over $\mathbb{F}_{2^m}$: an elementary derivation, *Bull. Polish Acad. Sci. Math.*, 59, 2011, pg. 11-18.

[21] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.*, Vol. 44, N. 170, 1985, pg. 483-494.

[22] L. Stickelberger, Ueber eine Verallgemeinerung der Kreistheilung, *Math. Ann.*, XXXVII Band, 3 Heft, 1890, pg. 321-367.

[23] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.

[24] A. Winterhof, On the Distribution of Powers in Finite Fields, *Finite Fields Appl.*, 4, 1998, pg. 43-54.